(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－344117

(43)公開日　平成５年(1993)12月24日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/06				
9/14				
Ｇ０９Ｃ　1/00		9194－5L		
		7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数４(全　７　頁)

(21)出願番号　特願平4－175912

(22)出願日　平成４年(1992)６月11日

(71)出願人　000001214
国際電信電話株式会社
東京都新宿区西新宿２丁目３番２号

(72)発明者　椿山　英樹
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　大橋　正良
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　古賀　敬一郎
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

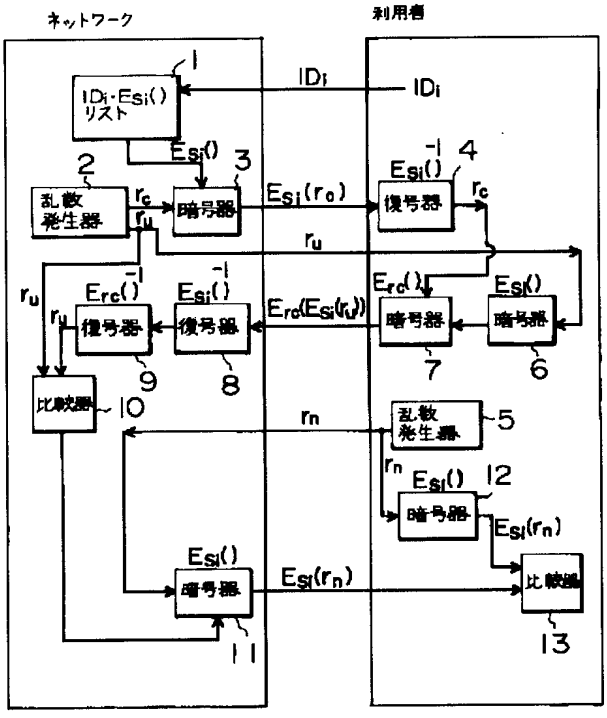
(74)代理人　弁理士　大塚　学

(54)【発明の名称】　相手認証／暗号鍵配送方式

(57)【要約】

【目的】利用者が自分のＩＤネットワークに呈示後、２度あるいは３度の通信のみでネットワークによる利用者の認証、利用者によるネットワークの認証、共通鍵の配送をすべて実現できるようにする。

【構成】通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、認証のためにネットワークから利用者へ送られるデータと、その後の秘密通信を行なうための暗号鍵を暗号化したデータを共に利用者へ送ることにより、利用者がまず自分の名前（ＩＤ）をネットワークに示した後、ネットワークと利用者間で多くとも３回の通信を行なうことにより、認証の完了および暗号通信のための暗号鍵の配信を完了させる。



1

【特許請求の範囲】

【請求項１】　通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、検証者から証明者に送る暗号化された乱数を証明者にて復号したものを暗号鍵として用い、検証者から送られてきた認証用の乱数を証明者が暗号化し、検証者に送り返すことにより利用暗号アルゴリズムに対する選択平文攻撃を不可能とする相手認証をおこなうことを特徴とする相手認証／暗号鍵配送方式。

【請求項２】　通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、検証者が証明者を認証するために発生し証明者に送る乱数および証明者が自分で発生した乱数を、特定の関数で処理した値を証明者が暗号化し検証者に送り返すことにより、利用暗号アルゴリズムに対する選択平文攻撃を不可能とする相手認証を行なうことを特徴とする相手認証／暗号鍵配送方式。

【請求項３】　通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、相手が自分を認証するためのデータと、自分が相手を認証するためのデータを同時に送ることにより、利用者がまず自分の名前（ＩＤ）をネットワークに示した後、ネットワークと利用者間で多くとも３回の通信を行なうことにより、ネットワークによる利用者の認証、利用者によるネットワークの認証を完了させることを特徴とする相手認証／暗号鍵配送方式。

【請求項４】　通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、

2

さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、認証のためにネットワークから利用者へ送られるデータと、その後の秘密通信を行なうための暗号鍵を暗号化したデータを共に利用者へ送ることにより、利用者がまず自分の名前（ＩＤ）をネットワークに示した後、ネットワークと利用者間で多くとも３回の通信を行なうことにより、認証の完了および暗号通信のための暗号鍵の配信を完了させることを特徴とする相手認証／暗号鍵配送方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信ネットワークの情報保全技術に係り、特にはパーソナル移動通信システムにおいてネットワークの不正利用を防ぐ相手認証／暗号鍵配送方式に係るものである。

【０００２】

【従来の技術】通信ネットワークにおいて、システムの情報保全を図る技術には大別して、(a) 利用者が正当かどうかを確認して不正なアクセスを防ぐ相手認証技術と、(b)実際に通信が行なわれている回線上の通信内容を秘匿して、第三者による盗聴を防止する暗号化技術がある。(a)の認証技術においては、ＣＣＩＴＴでは将来のパーソナル通信技術用の認証技術として、ネットワーク、利用者すべてに同一の暗号装置を用いて、パスワードのような個人の秘密情報を回線上に出すことなくネットワークが利用者を認証する図５に示すような方式が提案されている。即ち、利用者ｉのＩＤを$ＩＤ_i$、その秘密情報を$Ｓ_i$とし、$Ｓ_i$は利用者とネットワークのみが秘密に保持しているものとする。もし利用者ｉがネットワークを利用したいときには、まず$ＩＤ_i$をネットワークに示す。次にネットワークは乱数$ｒ_u$を発生して利用者ｉに送る。利用者ｉは暗号装置を用いて、秘密情報$Ｓ_i$を秘密鍵として$ｒ_u$を暗号化し、ネットワークに返す。最後にネットワークは自分で保持している利用者ｉの秘密情報を取り出して同じくこれを秘密鍵として$ｒ_u$を暗号化し、この値がｉから送ってきた値と一致すれば利用者ｉを正当な利用者として認証するという方式である。この方式では利用者のネットワークへのＩＤの呈示を含めて、利用者とネットワーク間で計３回の通信のやりとりが行なわれている。その後(b) を実現するために何らかの鍵配送方式を用いて、ネットワークと利用者の間で鍵共有を実現する。最後に共有された秘密の鍵を用いて通信文を暗号化し、両者間で通信を開始する。

【０００３】

【発明が解決しようとする課題】従来技術の項で述べたように、これまではネットワークが利用者を認証する機能にのみ主眼がおかれていた。これはネットワークは常に正しいという認識でシステムが設計されていた点による。しかしながらパーソナル通信においては、極く小さ

な通信範囲のみをカバーする基地局が利用者との通信や利用者の移動に伴う位置登録を行なうことが想定されるため、不正を働こうとするものが、偽の基地局を設けて無線回線を通じて利用者にアクセスすることが考えられる。このような事態が生じた場合、利用者は不正なネットワークが故意に選ぶ適当な数字を自分の秘密情報を鍵として暗号化し、不正ネットワークに送り返すことになる。これはいわゆる選択平文攻撃であり、暗号システムに対する各種攻撃のなかでももっとも強力なものである。暗号方式の選択によっては幾度かの選択平文攻撃により利用者の秘密情報が露呈する危険性が文献（E. Biham and A. Shamir:"Differential cryptoanalysis of DES-1 ike cryptosystems",'90 EUROCRYPTO, August 1990.）により指摘されている。また今後は一社のみならず複数の業者がパーソナル通信サービスを提供することが想定されるため、利用者は現在どの業者のサービスを受けているのかを正確に把握する必要がある。また、従来の方式では、暗号化通信を行なうために必要な鍵配送の為に、さらにネットワークと利用者の間でやり取りを行なう必要があった。

【０００４】本発明の目的は、上述した従来技術の問題点を解消して、ネットワークが利用者を認証すると共に、利用者もネットワークを認証し、さらに暗号通信のための鍵配送をも、ネットワーク－利用者間の少ないやり取りのなかでおこなうことができる相手認証／暗号鍵配送方式を提供することにある。

【０００５】

【課題を解決するための手段】前記課題の解決は、本発明の次に列挙する新規な特徴的構成手法を採用することにより達成される。即ち、本発明の第１の特徴は、通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、検証者から証明者に送る暗号化された乱数を証明者にて復号したものを暗号鍵として用い、検証者から送られてきた認証用の乱数を証明者が暗号化し、検証者に送り返すことにより利用暗号アルゴリズムに対する選択平文攻撃を不可能とする相手認証／暗号鍵配送方式である。

【０００６】本発明の第２の特徴は、通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、検証者が証明者を認証するために発生し証明者に送る乱数および証明者が自分で発生した乱数を、特定の関数で処理した値を証明者が暗号化し検証者に送り返すことにより、利用暗号アルゴリズムに対する選択平文攻撃を不可能とする相手認証／暗号鍵配送方式である。

【０００７】本発明の第３の特徴は、通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、相手が自分を認証するためのデータと、自分が相手を認証するためのデータを同時に送ることにより、利用者がまず自分の名前（ＩＤ）をネットワークに示した後、ネットワークと利用者間で多くとも３回の通信を行なうことにより、ネットワークによる利用者の認証、利用者によるネットワークの認証を完了させる相手認証／暗号鍵配送方式である。

【０００８】本発明の第４の特徴は、通信ネットワークおよびその全利用者に共通な共通鍵暗号方式を具現する装置が与えられている状況下で、各利用者にそれぞれ利用者名（ＩＤ）が割当てられ、ネットワーク内に公開されると同時に、共通鍵暗号の鍵として用いられるＩＤに付随した秘密情報がネットワークにより作成されて利用者に秘密に配付され、さらにネットワークのデータベース内にこれら全利用者のＩＤと秘密情報が保管されている場合において、認証のためにネットワークから利用者へ送られるデータと、その後の秘密通信を行なうための暗号鍵を暗号化したデータを共に利用者へ送ることにより、利用者がまず自分の名前（ＩＤ）をネットワークに示した後、ネットワークと利用者間で多くとも３回の通信を行なうことにより、認証の完了および暗号通信のための暗号鍵の配信を完了させる相手認証／暗号鍵配送方式である。

【０００９】

【実施例１】以下に図１及び図２を用いて本発明の第１の実施例を詳細に説明する。まず利用者ｉは自分の名前ID_iをネットワークに示す。次にネットワークは利用者認証用の乱数r_uと、ネットワークと利用者ｉとの通信に用いる共通鍵r_cを乱数発生器２から発生する。続いてネットワークは、利用者ｉの名前ID_iに基づき$ID_i - Es_i(\ )$リスト１から$Es_i(\ )$を発生し暗号器３から利用者ｉの秘密鍵S_iによって暗号化された出力$Es_i(r_c)$を作成し、r_uと$Es_i(r_c)$をｉに送る。このとき秘密鍵S_iを知っているｉのみが、$Es_i(r_c)$から暗号復号関数$E^{-1}s_i(\ )$を用いて、

復号器４から共通鍵r_cを得ることができる。これを受けて利用者ｉは、ネットワーク認証用の乱数r_nを乱数発生器５から発生する。次にｉはネットワークが用いたのと同じ暗号E_{s_i}（ ）を暗号器６で発生し、これを用いて、利用者の秘密鍵S_iによってr_uを暗号化してE_{s_i}（r_u）を作成し、さらに共通鍵r_cによってE_{s_i}（r_u）を暗号器７で暗号化してE_{r_c}（E_{s_i}（r_u））を作成し、r_nとE_{r_c}（E_{s_i}（r_u））をネットワークに送り返す。これを受けてネットワークは自分で保持しているr_u、共通鍵r_cおよびｉの秘密情報S_iからE_{r_c}（E_{s_i}（r_u））を計算し、この値がｉから送ってきた値と一致すればｉを正当な利用者として認証するか、あるいは暗号鍵S_iおよびr_cの暗号復号関数E_{s_i}（），E_{r_c}（）を用いることにより、利用者ｉから送られてきたE_{r_c}（E_{s_i}（r_u））を復号器８，９で復号しr_uを得、ネットワークが作成したr_uと比較器１０で比較して両者が一致すればｉを正当な利用者として認証する。もしもこの値が異なっていれば、利用者は正当なS_iを持っていないことから、ネットワークはこのセッションを切断する。その後ネットワークは正当と認められた利用者ｉに対して暗号器１１でE_{s_i}（r_n）を作成し、ｉに送り返す。ｉは乱数発生器５と暗号器１２を用いて自分で保持しているr_nおよびS_iからE_{s_i}（r_n）を計算し、この値がネットワークから送ってきた値と比較器１３で比較して一致すればネットワークを正当として認証するか、あるいは暗号鍵S_iの暗号復号関数E_{s_i}（ ）を用いることによりE_{s_i}（r_n）を復号しr_nを得、これが利用者が発生したものと一致すればネットワークを正当として認証する。もしもこの値が異なっていれば、ネットワークはデータベース中に利用者の正当なS_iを持っていないことから利用者はネットワークを不正と判断し、このセッションを切断する。このようにすれば、従来方式より一回の通信が多くなるだけで、即ちネットワークへのＩＤの呈示を含めて計４回の通信のやりとりを行なうのみで、(1) ネットワークによる利用者の認証、(2) 利用者によるネットワークの認証、(3) ネットワークから利用者への共通鍵の配信の３機能をすべて安全に実現することができる。

【００１０】さらに通信回数を少なくし、従来方式と同じネットワークへのＩＤの呈示を含めて計３回の通信のやりとりを行なうのみで(1) ネットワークによる利用者の認証、(2) 利用者によるネットワークの認証、(3) ネットワークから利用者への共通鍵の配信の３機能をすべて安全に実現することを可能とする第２の実施例を次に示す。

【００１１】

【実施例２】以下に図３及び図４を用いて本発明の第２の実施例を詳細に説明する。まず利用者ｉは、ネットワーク認証用の乱数r_nを発生する。利用者ｉは自分の名

前ID_iと乱数発生器２０で発生された認証用の乱数r_nをネットワークに示す。次にネットワークは利用者認証用の乱数r_uと、ネットワークと利用者ｉとの通信に用いる共通鍵r_cを乱数発生器２２により発生する。ネットワークは、認証情報処理関数器２３による関数Ｆ（ ）および利用者ｉの秘密鍵S_iによる共通鍵暗号関数E_{s_i}（ ）を用いて暗号器２４でE_{s_i}（Ｆ（r_c，r_n））を計算し、r_uとE_{s_i}（Ｆ（r_c，r_n））をｉに送る。次に利用者ｉは、利用者ｉの秘密鍵S_iによる復号器２５における復号関数である$E^{-1}{}_{s_i}$（ ）と認証情報処理逆関数器２６での関数Ｆ（ ）逆関数F^{-1}（ ）を用いて、$E^{-1}{}_{s_i}$（E_{s_i}（Ｆ（r_c，r_n））を計算し、（r_c，r_n）を得、r_cを暗号化通信用の共通鍵とする。また、利用者は、自分が送った認証用の乱数r_uと復号し得られたr_uが比較器２７での比較結果が一致すればネットワークを正当として認証する。もしもこの値が異なっていれば、ネットワークはデータベース中に利用者の正当なS_iを持っていないことから利用者はネットワークを不正と判断し、このセッションを切断する。ただし、利用者ｉの秘密鍵S_iによる復号関数を知っているのは利用者ｉと正しいネットワークのみである。従って、$E^{-1}{}_{s_i}$（ ）を知らない他人には、E_{s_i}（r_c，r_n）は意味不明の乱数にしか見えない。

【００１２】続いて利用者ｉは、利用者の秘密鍵S_iによってr_uを暗号器２９により暗号化してE_{s_i}（r_u）を作成し、E_{s_i}（r_u）をネットワークに送り返す。これを受けてネットワークは自分で保持しているr_uとｉの秘密情報S_iから暗号器２８でE_{s_i}（r_u）を計算し、この値とｉから送ってきた値とを比較器３０で比較した結果一致すればｉを正当な利用者として認証する。あるいは、ｉから送られてきたE_{s_i}（r_u）を、利用者ｉの秘密鍵S_iによる復号関数である$E^{-1}{}_{s_i}$（ ）を用いて、$E^{-1}{}_{s_i}$（E_{s_i}（r_u））を計算し、得られたが利用者ｉに送ったものと一致すればｉを正当な利用者と認証する。もしもこの値が異なっていれば、利用者は正当なS_iを持っていないことから、ネットワークはこのセッションを切断する。このようにすれば、ネットワークへのＩＤの呈示を含めて計３回の通信のやりとりを行なうのみで、(1) ネットワークによる利用者の認証、(2) 利用者によるネットワークの認証、(3) ネットワークから利用者への共通鍵の配信の３機能をすべて安全に実現することができる。

【００１３】なお、本例で用いた関数Ｆ（ ）は次の「関数Ｆ（ ）の条件」を満たす必要がある。

「関数Ｆ（ ）の条件」

条件１　ｘ，ｙが決定したとき、ｚ＝Ｆ（ｘ，ｙ）を満たすｚは一意に決定されること。

条件２　ｚが決定したとき、ｚ＝Ｆ（ｘ，ｙ）を満たすｘ，ｙは一意に決定されること。

条件３　あるｘが与えられ、ランダムなｒを確率的変数

7

とした時、Ｅｓｉ（Ｆ（ｒ，ｘ））の出力値を２進数展開した系列のどの一部をとっても固定のパターンとなる確率は小さいこと。

【００１４】

【発明の効果】本発明を用いると不正な利用者がネットワークを利用することを防ぐのみならず、不正なネットワークが利用者から鍵情報を盗みだそうとしてもその行為を防止できるため、システムの安全性を向上させる効果が大である。さらに、本発明では、利用暗号関数に対する選択平文攻撃を不可能としており、安全性を大幅に向上させている。しかも本方式は従来の共通鍵暗号技術で具備すべき暗号装置のみで実現できるうえに、通信回数も従来技術と全く同じか、あるいは一回多いだけでありながら、暗号通信のために必要となる暗号鍵の配信も同時に行なうことができる。したがって本発明を導入してもシステムに余分にかかる負担は極めて軽微であるといえるため、今後のネットワークセキュリティに寄与するところが大である。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示すブロック図である。

【図２】本発明の第１の動作を示すフローチャートである。

【図３】本発明の第２の実施例を示すブロック図である。

【図４】本発明の第２の動作を示すフローチャートである。

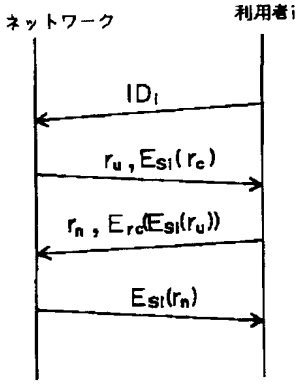
8

【図５】従来例の動作を示すフローチャートである。

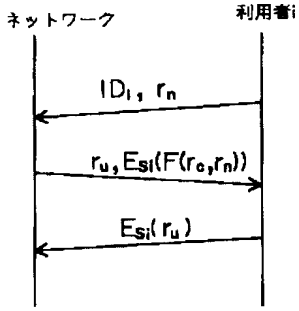
【符号の説明】

１　ＩＤｉ・Ｅｓｉ（）リスト
２　乱数発生器
３　暗号器
４　復号器
５　乱数発生器
６　暗号器
７　暗号器
８　復号器
９　復号器
１０　比較器
１１　暗号器
１２　暗号器
１３　比較器
２１　ＩＤｉ・Ｅｓｉ（）リスト
２２　乱数発生器
２３　認証情報処理関数器
２４　暗号器
２５　復号器
２６　認証情報処理逆関数器
２７　比較器
２８　暗号器
２９　暗号器
３０　比較器

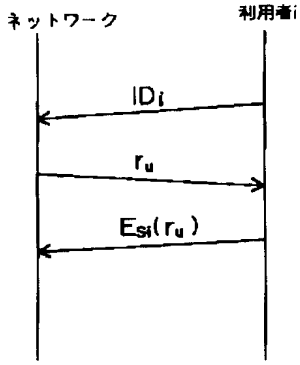
【図２】



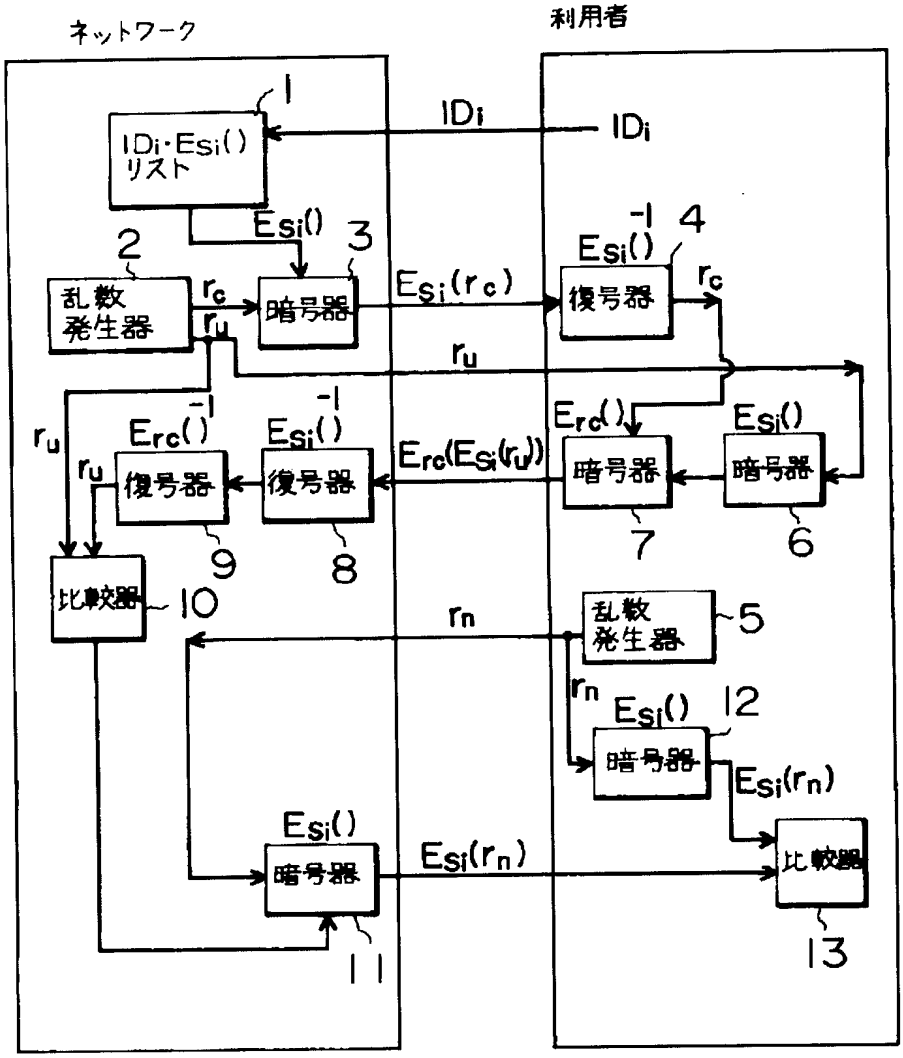
【図４】



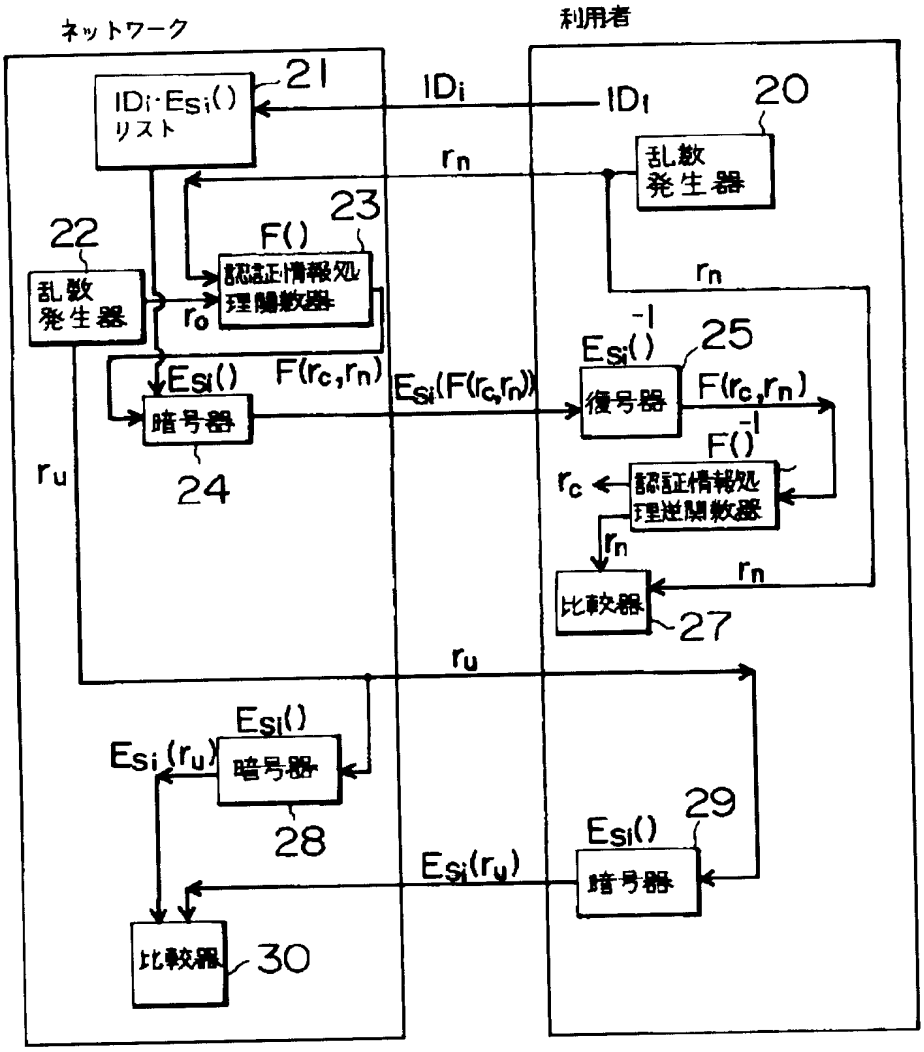
【図５】



【図１】


ネットワーク
利用者
IDi・Esi()リスト
1
IDi
IDi
Esi()
2
3
-1
4
乱数発生器
rc
ru
暗号器
Esi(rc)
復号器
rc
ru
ru
-1
-1
Erc()
Esi()
Erc()
Esi()
ru
ru
復号器
復号器
Erc(Esi(ru))
暗号器
暗号器
9
8
7
6
比較器
10
rn
乱数発生器
5
rn
Esi()
12
暗号器
Esi(rn)
Esi()
Esi(rn)
比較器
暗号器
11
13

【図３】


ネットワーク
利用者
IDi·Esi()
リスト
21
IDi
IDi
20
乱数
発生器
rn
23
F()
22
乱数
発生器
認証情報処理関数器
r0
rn
Esi()
暗号器
F(rc,rn)
Esi(F(rc,rn))
-1
Esi()
25
復号器
F(rc,rn)
-1
F()
認証情報処理逆関数器
rc
rn
rn
比較器
27
24
ru
ru
Esi()
Esi(ru)
暗号器
28
29
Esi()
Esi(ru)
暗号器
比較器
30